Computing In-Service Aircraft Reliability

Laurent Saintis, Emmanuel Hugues, Christian Bes, Marcel Mongeau

COMPUTING IN-SERVICE AIRCRAFT RELIABILITY

SAINTIS LAURENT

Airbus France, Aircraft Operability Division,

31060 Toulouse cedex 3, France

Laurent.saintis@free.fr

HUGUES EMMANUEL

Airbus France, Aircraft Operability Division,

31060 Toulouse cedex 3, France

emmanuel.hugues@airbus.com

BES CHRISTIAN

Laboratoire de Génie Mécanique de Toulouse, Université Paul Sabatier,

31062 Toulouse cedex 9, France

cbes@cict.fr

MONGEAU MARCEL

Université de Toulouse ; UPS, INSA, UT1, UTM ; Institut de Mathématiques de Toulouse ; F-31062 Toulouse, France.,

CNRS ; Institut de Mathématiques de Toulouse UMR 5219 ; F-31062 Toulouse, France

mongeau@math.univ-toulouse.fr

Received (Day Month Year)
Revised (Day Month Year)

This paper deals with the modeling and computation of in-service aircraft reliability at the preliminary design stage. This problem is crucial for aircraft designers because it enables them to evaluate in-service interruption rates, in view of designing the system and of optimizing aircraft support. In the context of a sequence of flight cycles, standard reliability methods are not computationally conceivable with respect to industrial timing constraints. In this paper, first we construct the mathematical framework of in-service aircraft reliability. Second, we use this model in

order to demonstrate recursive formulae linking the probabilities of the main failure events. Third, from these analytic developments, we derive relevent reliability bounds. We use these bounds to design an efficient algorithm to estimate operational interruption rate indicators. Finally, we show the usefulness of our approach on real-world cases provided by Airbus.

Keywords: Aircraft reliability, fault trees, reliability modeling, repairable system.

List of notation

ADM	Accepted Degraded Mode
BA	Bound Algorithm
DM	Degraded Mode
OI	Operational Interruption
OR	Operational Reliability
RDM	Refused Degraded Mode
NG	No Go dispatch condition on the system
T	Index of cycle
S	The (finite) set of all components within the system
n	Number of components in S
k	Number of minimal cuts
MC^i	i^{th} Minimal Cut, $1 \le i \le k$
MC_T^i	The event that all components of MC^i are failed at the end of cycle T
p	Number of minimal paths
MP^j	j^{th} Minimal Path, $1 \le j \le p$
MP_T^j	The event that all components of MP^j work at the end of cycle T
NG_T	The event that a No Go dispatch condition occurs during cycle T

xD_T The event that component x works at the Departure (beginning) of cycle T

xF_T The event that component x Fails during cycle T

ADM_T The event that the airline Accepts the Degraded Mode for take-off at the beginning of cycle $T+1$

RDM_T The event that the airline Refuses the Degraded Mode for take-off at the beginning of cycle $T+1$

$\overline{E}$ Complement of event E

$P\{E\}$ Probability of event E

$UB(E)$ Upper Bound for $P\{E\}$

$LB(E)$ Lower Bound for $P\{E\}$

k-out-of-n:F system An n-component system that fails if and only if at least k components fail

1. Introduction

In-service aircraft reliability relates to aircraft availability and punctuality. It measures the frequency of unscheduled service interruptions caused by technical failures and associated required maintenance. The different interruption types are:

- delays at take-off (the aircraft departs later than the scheduled departure time),
- flight cancellations (the aircraft does not depart at all),

- air diversions (the aircraft has to land at an airport different from its destination),
- in-flight turn-backs (the aircraft has to return to its departure airport).

For airlines, these unscheduled service interruptions induce high direct costs related to the aircraft: fuel consumption, airport taxes, flight crew accommodation / duty time, passenger accommodation, financial compensation, etc. They also induce high indirect costs: loss of image, impact on customer loyalty, etc. Thus, in-service aircraft reliability is closely monitored by airlines and, therefore, also by aircraft manufacturers. As a consequence, in-service aircraft reliability has become a major target for aircraft designers.

At the preliminary design stage, predicting accurate levels of an aircraft future in-service reliability is a key issue. This allows optimizing system design for targeted support performances. This prediction involves computing system failure probabilities, which requires the modeling and analysis of a dynamic process using a fault-tree analysis at each flight cycle[1]. Previous methods for computing these failure probabilities include the following: Markov processes[2], Monte-Carlo simulation, dynamic fault trees and multi-state systems. Because of the explosion of the number of possible states of the system, Markov processes[3] cannot be considered here. On the other hand, Monte-Carlo simulation[4,5] requires too many simulations to obtain sufficient precision. Indeed, in our context the interruption rate probability is between 10^{-7} and 10^{-4} per take-off. Despite recent progress on dynamic fault trees[6] and multi-state systems[7], these two approaches cannot be applied because the CPU time required to extract all the minimal sequences is unmanageable (there can be up to 1,600 flight cycles during one year of aircraft use). The lack of general tractable methods for large-scale dynamic models has yielded analytical developments for specific problems[8,9]. However, these results do not apply to our

aeronautical reliability problem, which involves a long sequence of flight cycles with dynamic dependencies between component states due to maintenance strategies.

The contribution of the present paper relates to three aspects of in-service aircraft reliability: modeling, efficient resolution, and validation. It is organized as follows. In Section 2, we develop the framework of the in-service aircraft reliability problem in the context of preliminary design. Our model describes both the different failure modes of an aircraft system during its successive flight and ground phases, and the way airlines manage these failures. In Section 3, we derive recursive formulae linking the probabilities of the main failure events. This allows us to construct an efficient algorithm that provides relevant bounds for operational interruption rate indicators that meets industrial time constraints. Section 4 reports computational experiments on a k-out-of-n:F system, on an Air Data Inertial Reference System, and on an aircraft refuel system. These results show the efficiency and precision of our approach. We conclude in Section 5.

2. Model Formulation

In this section, we first present the framework of the in-service aircraft reliability problem. Then, we list the input data and the assumptions of the model.

2.1. *Framework*

In service, an aircraft is subject to a sequence of cycles with each cycle consisting of a flight phase, followed by a ground phase (which then precedes the next flight). Here we consider an aircraft system made up of a number of various components. During any phase, a component failure may occur. Fig. 1 illustrates the main events that may occur in a sequence of cycles.

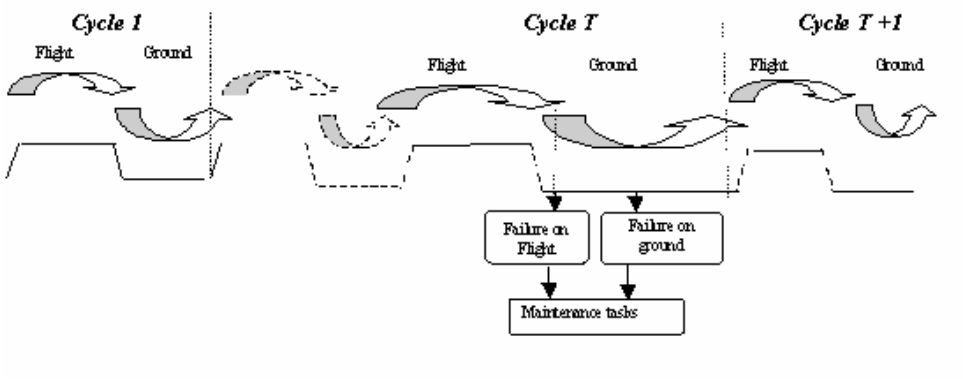

Fig. 1. Operational profile

When a component *x* fails during cycle *T*, it may cause the system not to meet the dispatch conditions (safety, operability, commercial...), so-called *No Go dispatch conditions* (NG). Formally the occurrence of a NG event is represented by a fault tree, which is based solely on the component states (working or failed). In the case of NG during cycle *T*, the airline must repair *all* the components in a state of failure. When a component *x* fails without involving NG, then two decisions can be made by the airline. Either the airline decides to take off in a so-called *Accepted Degraded Mode* (ADM), or it refuses the degraded mode (RDM), and then repairs the component that has just failed during cycle *T*, and does not repair any previously failed component. Note that if a degraded mode is accepted, some minor maintenance tasks configure the component that has just failed. Fig. 2 illustrates all of these different scenarios in detail.

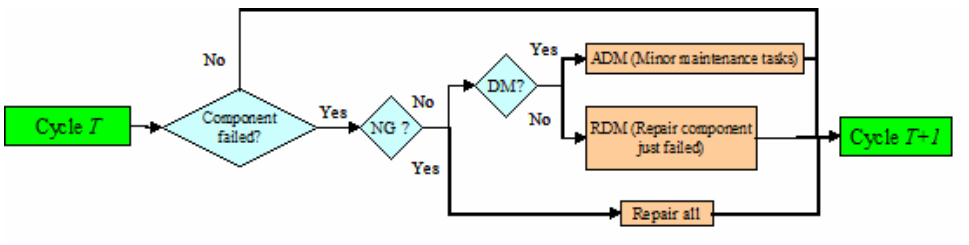

Fig. 2. The different possible scenarios during a cycle

From the two possible states of any given component x at the departure of cycle T: x works (xD_T) or x is failed ($\overline{xD_T}$), we display in Fig. 3 all the events that may occur within cycle T.

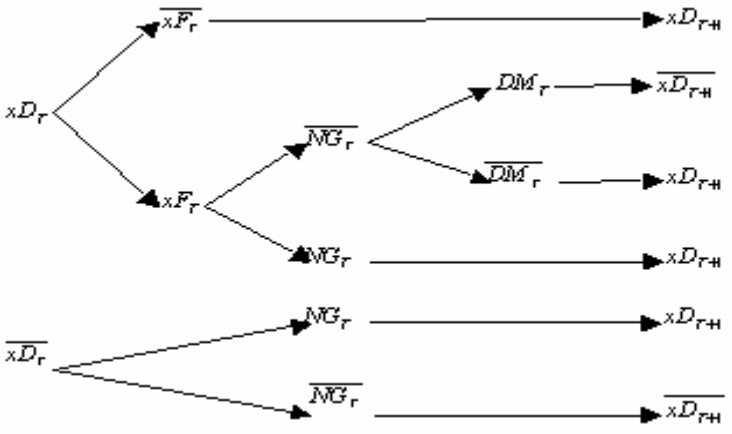

Fig. 3. The event tree for component x during cycle T.

2.2. *Input data*

Here is the input data (known quantities) of the in-service aircraft reliability problem:

- A coherent fault tree of the system. This fault tree is issued from the system architecture by design engineers.
- $\Pr\{xF_T | xD_T\}$, the probability that component x fails during cycle T, given that x works at the beginning of cycle T. This quantity is a direct function of the failure rate of component x, which is provided by the component manufacturer.
- $\Pr\{ADM_T | \overline{NG_T} \cap xF_T \cap xD_T\}$, the probability of accepting the degraded mode, given that x fails during cycle T and that no NG_T (i.e. $\overline{NG_T}$) occurs. This quantity is a direct function of the pilot behavior and of the airline

maintenance strategy. It is *not* a function of the component (see Assumption A7 below).

Note that, due to NG_T event, ADM_T (Accepted Degraded Mode) is *not* the complement event of RDM_T (Refused Degraded Mode). However, ADM_T and RDM_T are *conditional* complement events, more precisely:

$$\Pr\left\{ADM_T \middle| \overline{NG_T} \cap xF_T \cap xD_T\right\} = 1 - \Pr\left\{RDM_T \middle| \overline{NG_T} \cap xF_T \cap xD_T\right\}.$$

- The initial conditions are also given: we know the state or the probability $\Pr\{xD_1\}$ of each component *x* at the beginning of cycle 1.

2.3. *List of assumptions*

Here, we list the assumptions induced by both the airline maintenance strategy and the reliability of aircraft systems.

A1. Given the states (working or failed) of each component at the beginning of the cycle *T*, the component probabilities of failure are independent.

More precisely, the conditional probabilities of failure are independent while non-conditional probabilities of failure are not. In fact the dependencies between failure events are due to the NG event occurrence.

A2. The probability of having more than one component failure during each cycle for the system under study is negligible.

Indeed, because our reliability study is dedicated to operational interruption rate evaluation and due to the fact that we have to deal with highly reliable components, the above probability is negligible compared with standard targets for operational interruption rates (see also Ref. 10 for detail on this

assumption). This fact is also confirmed by operational interruption rate estimation throughout airline maintenance data.

A3. A component *x* is repaired at cycle *T* only in the following cases:

a. NG occurs during cycle *T* and component *x* was in failed state at the departure of cycle *T*

b. Component *x* fails during cycle *T* and NG occurs during cycle *T*.

c. Component *x* fails during cycle *T*, NG does not occur during cycle *T* and the airline refuses the degraded mode for the *x* component.

A4. When a component is repaired during cycle *T*, it is assumed to be working at the departure of cycle *T+1*.

A5. In the cases of NG during cycle *T*, all the equipments failed before or during cycle *T* are repaired.

A6. The degraded mode acceptance by the airline during cycle *T* (ADM_T) can occur when both a component fails and NG does not occur during cycle *T*. Once a degraded mode has been accepted for component *x*, *it* remains failed unless NG occurs during the following cycles.

A7. Given that a component has failed during cycle *T* without inducing NG, we assume that ADM_T (the degraded mode acceptance event) is independent of both *x* (the component) and *T* (the cycle).

Remark that his conditional probability quantity is in practice given by the airline maintenance strategy and by the pilot behavior. Note that due to the NG coupling effect, the non-conditional probability of the degraded mode acceptance depends upon cycle T, but is independent of the failed component.

A8. The airline refuses degraded mode during cycle T (RDM_T) can occur when both a component fails and NG does not occur during cycle T. Once a degraded mode has been refused for component x, *it* is repaired and it is assumed to be working at the beginning of cycle $T+1$.

A9. Given that a component has failed during cycle T without inducing NG, we assume that RDM_T (the event that the airline refuses the degraded mode) is independent of both x and T.

The strictly analogous remark of A7 for ADM_T applies also here for RDM_T.

A10. The component failure rates are supposed to be different but independent of the cycle (constant through the sequence of cycles).

A11. We assume the following **negative dependency property:** at the departure of cycle T, the probability that both components x and y are in failed state is smaller than the individual probability product. More formally, let $x, y \in S, x \neq y$ be two components. Then,

$$\Pr\{\overline{xD_T} \cap \overline{yD_T}\} \leq \Pr\{\overline{xD_T}\} \times \Pr\{\overline{yD_T}\}.$$

As a direct consequence, we have the following general result: Let $x \in S$ and A a subset of the remaining components ($A \subset S$ with $x \notin A$). Then,

$$\Pr\left\{\overline{xD_T} \cap \left(\bigcap_{y \in A}\left(\overline{yD_T}\right)\right)\right\} \leq \Pr\{\overline{xD_T}\} \times \Pr\left\{\bigcap_{y \in A}\left(\overline{yD_T}\right)\right\}.$$

Remark: this negative dependency assumption is also equivalent to:

For all pairs of components $x, y \in S$ ($x \neq y$):

$$\Pr\{xD_T \cap yD_T\} \leq \Pr\{xD_T\} \times \Pr\{yD_T\}.$$

The negative dependency property is a consequence of both the maintenance strategy (see Fig. 2), and the fact that we deal with highly reliable components (see Appendix for a detailed justification).

3. From analytic developments to efficient computation

The objective of this section is to compute at each cycle T estimates of the probabilities of the main events displayed on Fig. 2: NG (No Go dispatch condition on the system), ADM (Accepted Degraded Mode), and RDM (Refused Degraded Mode), which are in-service aircraft reliability indicators at the preliminary design stage. We present our methodology for computing these probabilities in four steps. In Subsection 3.1, we develop recursive analytical formulae (from cycle T to cycle $T+1$) for the three main-event probabilities $\Pr\{NG_T\}, \Pr\{ADM_T\}$, and $\Pr\{RDM_T\}$. However, these formulae rely on two probabilities that are not computationally tractable for real-world aeronautical systems. Thus, in Subsection 3.2 we develop astute bounds on probabilities related to minimal sets of the NG fault tree. These bounds, in turn, allow us in Subsection 3.3 to derive a bounding methodology for the above conditional NG event probabilities. Finally, we put these results together in Subsection 3.4 to derive an overall iterative scheme based on the initial conditions (at cycle T=1) and input data, in order to obtain an algorithm, called BA, for computing tight bounds for the three main-event probabilities. This algorithm does not rely on dynamic fault-tree analysis, and therefore it meets industrial computational time constraints for the systems considered in preliminary design.

3.1. *Probabilities of the main events: recursive formulae*

In this subsection, assuming that probability $\Pr\{xD_T\}$ is given for all components *x* in *S*, we show how to obtain, from this information, analytic formulae of the main-event probabilities: $\Pr\{NG_T\}$, $\Pr\{ADM_T\}$, $\Pr\{RDM_T\}$, and consequently $\Pr\{xD_{T+1}\}$ for all *x* in *S*. The latter probability will enable us to restart the iterative process.

When a NG occurs during cycle *T*, a component must have failed during this cycle. Therefore, we have:

$$NG_T = \bigcup_{x\in S}\left(NG_T \cap xF_T \cap xD_T\right).$$

Because the events $\{xF_T\}_{x\in S}$ are disjoint (see Assumption A2), we obtain:

$$\Pr\{NG_T\} = \sum_{x\in S}\Pr\{NG_T \,|\, xF_T \cap xD_T\}\times\Pr\{xF_T \,|\, xD_T\}\times\Pr\{xD_T\}. \qquad (1)$$

Similarly, for the second main event ADM_T, we have:

$$ADM_T = \bigcup_{x\in S}\left(ADM_T \cap \overline{NG_T} \cap xF_T \cap xD_T\right) \quad \text{(see Fig. 3).}$$

This implies

$$\Pr\{ADM_T\} = \sum_{x\in S}\Pr\{ADM_T \,|\, \overline{NG_T} \cap xF_T \cap xD_T\}\times\left(1-\Pr\{NG_T \,|\, xF_T \cap xD_T\}\right)\times\Pr\{xF_T \,|\, xD_T\}\times\Pr\{xD_T\}$$

. (2)

Again, from Fig. 3, $RDM_T = \bigcup_{x\in S}\left(RDM_T \cap \overline{NG_T} \cap xF_T \cap xD_T\right)$ and therefore:

$$\Pr\{RDM_T\} = \sum_{x\in S}\Pr\{\overline{ADM_T} \,|\, \overline{NG_T} \cap xF_T \cap xD_T\}\times\left(1-\Pr\{NG_T \,|\, xF_T \cap xD_T\}\right)\times\Pr\{xF_T \,|\, xD_T\}\times\Pr\{xD_T\}$$

. (3)

Finally, in accordance with Fig. 3, we have:

$$\overline{xD_{T+1}} = \left(\overline{xD_T} \cap \overline{NG_T}\right)\cup\left(ADM_T \cap \overline{NG_T} \cap xF_T \cap xD_T\right).$$

Hence, the probability of component *x* not working at the next cycle, *T+1*, is:

$$\Pr\{\overline{xD_{T+1}}\} = \Pr\{\overline{xD_T}\} - \Pr\{NG_T \cap (\overline{xD_T})\} + \Pr\{ADM_T \mid \overline{NG_T} \cap xF_T \cap xD_T\} \times (1 - \Pr\{NG_T \mid xF_T \cap xD_T\}) \times \Pr\{xF_T \mid xD_T\} \times \Pr\{xD_T\}. \quad (4)$$

Except for $\Pr\{NG_T \cap \overline{xD_T}\}$ and $\Pr\{NG_T \mid xF_T \cap xD_T\}$, all values involved in the above formulae are known from inputs (see Subsection 2.2) and from the given probabilities $\Pr\{xD_T\}_{x \in S}$. The next two subsections will address the issue of bounding / approximating these two unknown probabilities.

3.2. *Bounds related to minimal set probabilities*

The first step for bounding the two unknown probabilities $\Pr\{NG_T \cap \overline{xD_T}\}$ and $\Pr\{NG_T \mid xF_T \cap xD_T\}$, is to exhibit, for each minimal cut set MC^i and for each minimal path set MP^j, upper bounds on events MC_T^i (all components of MC^i are failed at the end of cycle *T*) and on events MP_T^j (all components of MP^j work at the end of cycle *T*). More precisely, we derive two types of recursive bounds. The first type is related to minimal cuts. In Theorem 1 below, we provide bounds on $\Pr\{MC_T^i \mid xF_T \cap xD_T\}$ and $\Pr\{MC_T^i \cap yF_T \cap yD_T \cap \overline{xD_T}\}$ for all i, $1 \le i \le k$, and for all components $x, y \in S,\ y \ne x$. The second type of recursive bounds, given by Theorem 2, relates to minimal paths and provides bounds on $\Pr\{MP_T^j \mid xF_T \cap xD_T\}$ and $\Pr\{MP_T^j \cap yF_T \cap yD_T \cap \overline{xD_T}\}$ for all j, $1 \le j \le p$, and for all components $x, y \in S,\ y \ne x$. All the upper bounds given by Theorems 1 and 2 can be computed

from input data and probabilities $\Pr\{xD_T\}$, $x \in S$. These bounds will be used in Subsection 3.3 in order to estimate the two unknown probabilities $\Pr\{NG_T \cap \overline{xD_T}\}$ and $\Pr\{NG_T | xF_T \cap xD_T\}$.

Theorem 1.

Consider the i[th] minimal cut, $1 \le i \le k$, and two components $x, y \in S$ with $x \neq y$. We then obtain:

i) $$\Pr\{MC_T^i | xF_T \cap xD_T\} \le \begin{cases} \dfrac{\prod\limits_{\substack{y \in MC^i \\ y \neq x}} \Pr\{\overline{yD_T}\}}{\Pr\{xD_T\}}, & if\ x \in MC^i \\ 0, & otherwise; \end{cases}$$

ii)

$$\Pr\{MC_T^i \cap yF_T \cap yD_T \cap \overline{xD_T}\} \le \begin{cases} \Pr\{yF_T | yD_T\} \times \left(\prod\limits_{\substack{z \in MC^i \\ z \neq x,\ z \neq y}} \Pr\{\overline{zD_T}\} \right) \times \Pr\{\overline{xD_T}\}, & if\ y \in MC^i \\ 0, & otherwise. \end{cases}$$

Proof.

Let us consider the event that all components of the minimal cut MC^i are in failed state during cycle *T*. If $x \in MC^i$ and *x* has failed during cycle *T*, following Assumption A2, we neglect the event that more than one component fail during one phase, and then, we assume that all the other components of this minimal cut have failed before. Thus, we have:

If we consider the **minimal cuts** for a cut MC^i to occur at *T*, a component $x \in MC^i$ must fail during the current cycle (only one according to Assumption A2), and the other components have to be lost at the beginning of the cycle *T*. Thus, this event can be rewritten as

$$MC_T^i \cap xF_T \cap xD_T = \begin{cases} \left(\bigcap_{\substack{y \in MC^i \\ y \neq x}} \overline{yD_T} \right) \cap xF_T \cap xD_T, & if\ x \in MC^i \\ \varnothing, & otherwise. \end{cases}$$

Let $x \in MC^i$,

$$\Pr\left\{MC_T^i \cap xF_T \cap xD_T\right\} = \Pr\left\{\left(\bigcap_{\substack{y \in MC_i \\ y \neq x}} \overline{yD_T} \right) \cap xF_T \cap xD_T\right\}$$

$$= \Pr\left\{xF_T \left| \left(\bigcap_{\substack{y \in MC_i \\ y \neq x}} \overline{yD_T} \right) \cap xD_T \right.\right\} \times \Pr\left\{\left(\bigcap_{\substack{y \in MC_i \\ y \neq x}} \overline{yD_T} \right) \cap xD_T\right\}.$$

The fact that $\Pr\left\{xF_T \left| xD_T \cap \left(\bigcap_{\substack{y \in MC_i \\ y \neq x}} \overline{yD_T} \right) \right.\right\} = \Pr\left\{xF_T \middle| xD_T\right\}$ is due to the probability independence of failure (A1).

We use the inclusion of events $\left(\bigcap_{\substack{y \in MC^i \\ y \neq x}} \overline{yD_T} \right) \cap xD_T \subseteq \left(\bigcap_{\substack{y \in MC^i \\ y \neq x}} \overline{yD_T} \right)$ and the overvaluation of their probabilities that can be deduced. Hence, with Assumption A11 (negative dependency) we obtain:

$$\Pr\left\{MC_T^i \cap xF_T \cap xD_T\right\} \le \Pr\left\{xF_T \mid xD_T\right\} \times \Pr\left\{\left(\bigcap_{\substack{y \in MC_i \\ y \neq x}} \overline{yD_T}\right)\right\}$$

$$\le \Pr\left\{xF_T \mid xD_T\right\} \times \prod_{\substack{y \in MC_i \\ y \neq x}} \Pr\left\{\overline{yD_T}\right\}$$

Consequently, with the equality

$\Pr\left\{MC_T^i \cap xF_T \cap xD_T\right\} = \Pr\left\{MC_T^i \mid xF_T \cap xD_T\right\} \times \Pr\left\{xF_T \cap xD_T\right\}$, we conclude.

ii) An analogous development of the previous proof is used to demonstrate the second overvaluation.

Let $y \notin MC^i$, $x \in S$. The cut cannot occur and we have:

$MC_T^i \cap yF_T \cap yD_T \cap \overline{xD_T} = \varnothing$.

Let $y \in MC^i$, $x \in S$. The cut will occur if all the other components are in a failure state at the beginning of the cycle. Thus, we have:

$$MC_T^i \cap yF_T \cap yD_T \cap \overline{xD_T} = \left(\bigcap_{\substack{z \in MC^i \\ z \neq x, z \neq y}} \overline{zD_T}\right) \cap yF_T \cap yD_T \cap \overline{xD_T}$$

Hence, if $y \in MC^i$, $x \in S$,

$$\Pr\left\{MC_T^i \cap yF_T \cap yD_T \cap \overline{xD_T}\right\} = \Pr\left\{ yF_T \left| \bigcap_{\substack{z\in MC^i \\ z\neq x, z\neq y}} \overline{zD_T} \cap yD_T \cap \overline{xD_T} \right. \right\} \times \Pr\left\{ \bigcap_{\substack{z\in MC^i \\ z\neq x, z\neq y}} \overline{zD_T} \cap yD_T \cap \overline{xD_T} \right\}$$

$$\leq \Pr\left\{yF_T \middle| yD_T\right\} \times \Pr\left\{ \bigcap_{\substack{z\in MC^i \\ z\neq x, z\neq y}} \overline{zD_T} \cap \overline{xD_T} \right\}.$$

The previous development relies on the fact that

$$\Pr\left\{ yF_T \left| \bigcap_{\substack{z\in MC^i \\ z\neq x, z\neq y}} \overline{zD_T} \cap yD_T \cap \overline{xD_T} \right. \right\} = \Pr\left\{yF_T \middle| yD_T\right\}$$ (from the probability independence of failures), and on the inclusion of the following events

$$yD_T \cap \left(\bigcap_{\substack{z\in MC^i \\ z\neq y}} \overline{zD_T} \right) \cap \overline{xD_T} \subset \left(\bigcap_{\substack{z\in MC^i \\ z\neq x, z\neq y}} \overline{zD_T} \right) \cap \overline{xD_T} \ .$$

Hence, with Assumption A11 (negative dependency) we conclude:

$$\Pr\left\{MC_T^i \cap yF_T \cap yD_T \cap \overline{xD_T}\right\} \leq \Pr\left\{yF_T \middle| yD_T\right\} \times \left(\prod_{\substack{z\in MC^i \\ z\neq x, z\neq y}} \Pr\left\{\overline{zD_T}\right\} \right) \times \Pr\left\{\overline{xD_T}\right\}. \ \square$$

Theorem 2.

Consider the j[th] minimal path, $1 \leq j \leq p$, and two components $x, y \in S$ with $x \neq y$.

Then, we have:

i) $$\Pr\left\{MP_T^j \middle| xF_T \cap xD_T\right\} \leq \begin{cases} 0, & if\ x \in MP^j \\ \prod_{y\in MP^j} \Pr\{yD_T\}, & otherwise. \end{cases}$$

ii)

$$\Pr\left\{MP_T^j \cap yF_T \cap yD_T \cap \overline{xD_T}\right\}$$
$$\leq \begin{cases} 0, & \text{if } x \in MP^j \text{ or } y \in MP^j \\ \min\left(\Pr\{yF_T \mid yD_T\} \times \left(\prod_{z \in MP^j} \Pr\{zD_T\}\right) \times \Pr\{yD_T\}, \Pr\{yF_T \mid yD_T\} \times \Pr\left\{\overline{xD_T}\right\}\right), & \text{otherwise.} \end{cases}$$

Proof.

i) If we consider the **minimal paths**, we exploit the observation that one component must fail during the current cycle in order to prevent all minimal paths from occurring. Again, using Assumption A2, the other components necessarily work at the beginning of the cycle. Thus, for any component $x \in S$, we have:

$$MP_T^j \cap xF_T \cap xD_T = \begin{cases} \varnothing, & \text{if } x \in MP^j \\ \left(\bigcap_{y \in MP^j} yD_T\right) \cap xF_T \cap xD_T, & \text{otherwise.} \end{cases}$$

The next development relies on (the remark in) Assumption A11, and on the fact that $\Pr\left\{xF_T \mid xD_T \cap \left(\bigcap_{y \in MP^j} yD_T\right)\right\} = \Pr\{xF_T \mid xD_T\}$ (from the probability independence of failures, Assumption A1):

$$\Pr\left\{MP_T^j \cap xF_T \cap xD_T\right\} \leq \begin{cases} 0, & \text{if } x \in MP^j, \\ \Pr\{xF_T \mid xD_T\} \times \left(\prod_{y \in MP^j} \Pr\{yD_T\}\right) \times \Pr\{xD_T\}, & \text{otherwise.} \end{cases}$$

ii) We use a development analogous to that of the previous proof to demonstrate the second overvaluation.

The event is divided as follows:

$$MP_T^j \cap yF_T \cap yD_T \cap \overline{xD_T} = \begin{cases} \varnothing, & \text{if } x \in MP^j \text{ or } y \in MP^j \\ \left(\bigcap_{z \in MP^j} zD_T \right) \cap yF_T \cap yD_T \cap \overline{xD_T} & \text{otherwise,} \end{cases}$$

but we cannot apply Assumption A11 to conclude directly.

On the other hand, with $x, y \notin MP^j$, we have the following two inclusions:

$$MP_T^j \cap yF_T \cap yD_T \cap \overline{xD_T} \subseteq \left(\bigcap_{z \in MP^j} zD_T \right) \cap yF_T \cap yD_T,$$

$$MP_T^j \cap yF_T \cap yD_T \cap \overline{xD_T} \subseteq yF_T \cap yD_T \cap \overline{xD_T}.$$

From the first inclusion, with (the remark in) Assumption A11, we obtain the following overvaluation:

$$\Pr\left\{MP_T^j \cap yF_T \cap yD_T \cap \overline{xD_T}\right\} \leq \Pr\left\{yF_T \middle| yD_T\right\} \times \left(\prod_{z \in MP^j} \Pr\{zD_T\} \right) \times \Pr\{yD_T\}.$$

From the second one, we use the inclusion $yD_T \cap \overline{xD_T} \subset \overline{xD_T}$ to obtain the following overvaluation:

$$\Pr\left\{MP_T^j \cap yF_T \cap yD_T \cap \overline{xD_T}\right\} \leq \Pr\left\{yF_T \middle| yD_T \cap \overline{xD_T}\right\} \times \Pr\left\{yD_T \cap \overline{xD_T}\right\} \leq \Pr\left\{yF_T \middle| yD_T\right\} \times \Pr\left\{\overline{xD_T}\right\}$$

We take the minimum of both overvaluations to conclude. □

Remark: For highly reliable systems, the second overvaluation is more efficient than the first one. It corresponds to the following inequality:

$$\Pr\{yD_T\} \times \prod_{z \in MP^j} \Pr\{zD_T\} \geq \Pr\left\{\overline{xD_T}\right\}.$$

3.3. *Bounds related to No Go dispatch condition probabilities*

Here, we show how to bound the unknown probabilities $\Pr\{NG_T \cap \overline{xD_T}\}$ and $\Pr\{NG_T | xF_T \cap xD_T\}$ of Subsection 3.1. More precisely, upper bounds will be derived in Theorem 3, using a minimal cut-set decomposition and Theorem 1 (Subsection 3.2). Then, using a minimal path-set decomposition and using Theorem 2 (Subsection 3.2), we shall derive lower bounds in Theorem 4. Note that all the bounds on $\Pr\{NG_T \cap \overline{xD_T}\}$ and $\Pr\{NG_T | xF_T \cap xD_T\}$ given by Theorems 3 and 4 can be computed from input data and the probabilities $\Pr\{xD_T\}$, $x \in S$.

Theorem 3.

For any component $x \in S$, we have:

i) $$\Pr\{NG_T | xF_T \cap xD_T\} \leq \sum_{i=1}^{k} \frac{\prod_{\substack{y \in MC^i \\ y \neq x}} \Pr\{\overline{yD_T}\}}{\Pr\{xD_T\}} \times 1_{\{x \in MC^i\}}, \qquad (5)$$

where $1_{\{x \in MC^i\}} := \begin{cases} 1 & if\ x \in MC^i, \\ 0 & otherwise. \end{cases}$

ii)

$$\Pr\{NG_T \cap \overline{xD_T}\} \leq \Pr\{\overline{xD_T}\} \times \left(\sum_{\substack{y \in S \\ y \neq x}} \Pr\{yF_T | yD_T\} \times \left(\sum_{i=1}^{k} \frac{\prod_{\substack{z \in MC^i \\ z \neq x \\ z \neq y}} \Pr\{\overline{zD_T}\}}{\Pr\{yD_T\}} 1_{\{y \in MC^i\}} \right) \right). \qquad (6)$$

Proof.

i) Let us consider the failure of a component x. In order to have a NG, at least one minimal cut which contains x must occur. Thus, using the general addition theorem bound and the fact that $NG_T = \bigcup_{i=1}^{k} MC_T^i$, we have, for any component $x \in S$:

$$\begin{aligned}\Pr\{NG_T \mid xF_T \cap xD_T\} &= \Pr\left\{\bigcup_{i=1}^{k} MC_T^i \,\middle|\, xF_T \cap xD_T\right\} \\ &\le \sum_{i=1}^{k} \Pr\{MC_T^i \mid xF_T \cap xD_T\} \\ &\le \sum_{i=1}^{k} \Pr\{MC_T^i \mid xF_T \cap xD_T\} \times 1_{\{x \in MC^i\}}.\end{aligned}$$

Hence, from Theorem 1, we obtain an upper bound for the NG probability given failure of a component $x \in S$ during cycle T:

$$\Pr\{NG_T \mid xF_T \cap xD_T\} \le \sum_{i=1}^{k} \frac{\prod_{\substack{y \in MC^i \\ y \ne x}} \Pr\{\overline{yD_T}\}}{\Pr\{xD_T\}} \times 1_{\{x \in MC^i\}}.$$

Of course, we can also obtain an upper bound for the NG probability using the previous overvaluation and Eq. (1).

ii) Based on formulation (1) of NG_T event, an analogous development can be applied to the event $NG_T \cap \overline{xD_T}$ to obtain the following overvaluation:

$$NG_T \cap \overline{xD_T} = \bigcup_{\substack{y \in S \\ y \ne x}} \left(yF_T \cap yD_T \cap NG_T \cap \overline{xD_T}\right).$$

$$\Pr\left\{NG_T \cap \overline{xD_T}\right\} = \sum_{\substack{y \in S \\ y \neq x}} \Pr\left\{yF_T \cap yD_T \cap NG_T \cap \overline{xD_T}\right\}$$

$$= \sum_{\substack{y \in S \\ y \neq x}} \Pr\left\{\bigcup_{i=1}^{k} \left(MC_T^i \cap yF_T \cap yD_T \cap \overline{xD_T}\right)\right\}$$

$$\leq \sum_{\substack{y \in S \\ y \neq x}} \sum_{i=1}^{k} \Pr\left\{MC_T^i \cap yF_T \cap yD_T \cap \overline{xD_T}\right\}$$

$$\leq \sum_{\substack{y \in S \\ y \neq x}} \Pr\left\{yF_T \middle| yD_T\right\} \times \Pr\left\{\overline{xD_T}\right\} \times \left(\frac{\prod_{\substack{z \in MC^i \\ z \neq x,y}} \Pr\left\{\overline{zD_T}\right\}}{\Pr\left\{yD_T\right\}} \right) \times 1_{\left\{y \in MC^i\right\}},$$

with the remarks:

- $\Pr\left\{yF_T \middle| yD_T \cap NG_T \cap \overline{xD_T}\right\} = \Pr\left\{yF_T \middle| yD_T\right\}$
- $yD_T \cap \overline{xD_T} \subset \overline{xD_T}$, which implies the overvaluation.

□

Theorem 4.

For any component $x \in S$, we have:

i) $$\Pr\left\{NG_T \middle| xF_T \cap xD_T\right\} \geq 1 - \sum_{j=1}^{p} \left(\prod_{y \in MP^j} \Pr\left\{yD_T\right\} \right) \times 1_{\left\{x \notin MP^j\right\}} \qquad (7)$$

ii)

$$\Pr\left\{NG_T \cap \overline{xD_T}\right\}$$
$$\geq \sum_{\substack{y\in S \\ y\neq x}} \Pr\left\{yF_T \middle| yD_T\right\} \times \Pr\left\{yD_T\right\} \times \Pr\left\{\overline{xD_T}\right\}$$
$$- \sum_{\substack{y\in S \\ y\neq x}} \sum_{\substack{j=1 \\ x,y\notin MP^i}}^{p} \left(\begin{array}{l} \min\left(\Pr\left\{yF_T \middle| yD_T\right\} \times \left(\prod_{z\in MP^j} \Pr\left\{zD_T\right\} \right) \times \Pr\left\{yD_T\right\}, \Pr\left\{yF_T \middle| yD_T\right\} \times \Pr\left\{\overline{xD_T}\right\} \right) \\ \times 1_{\left\{y\in MP^j\right\}} \times 1_{\left\{x\in MP^j\right\}} \end{array} \right). \tag{8}$$

Proof.

Let us consider the failure of a component *x*. In order to have a NG, all the minimal paths not containing *x*, do not occur at the beginning of the cycle.

i) If we consider the failure of a component *x*, to have a NG, Thus, using the general addition theorem bound and the fact that $NG_T = \bigcap_{j=1}^{p} \overline{MP_T^j}$, we have for any component $x \in S$:

$$\Pr\left\{NG_T \middle| xF_T \cap xD_T\right\} = \Pr\left\{ \bigcap_{j=1}^{p} \overline{MP_T^j} \middle| xF_T \cap xD_T \right\}$$
$$= 1 - \Pr\left\{ \bigcup_{j=1}^{p} MP_T^j \middle| xF_T \cap xD_T \right\}$$
$$\geq 1 - \sum_{j=1}^{p} \Pr\left\{MP_T^j \middle| xF_T \cap xD_T\right\}.$$

Hence, from Theorem 2, we obtain an upper bound for the NG probability given failure of a component $x \in S$ during cycle *T*:

$$\Pr\{NG_T \,|\, xF_T \cap xD_T\} \geq 1 - \sum_{j=1}^{p} \left(\prod_{y \in MP^j} \Pr\{yD_T\} \right) \times 1_{\{x \notin MP^j\}}.$$

ii) Based on formulation of NG event from Eq. (1) of the NG event, an analogous argument can be applied to the event $NG_T \cap \overline{xD_T}$ to obtain the following development:

$$NG_T \cap yF_T \cap yD_T \cap \overline{xD_T} = \left(\bigcap_{\substack{j=1 \\ x,y \notin MP_T^j}}^{p} \overline{MP_T^j} \right) \cap yF_T \cap yD_T \cap \overline{xD_T}\ .$$

From the fact that $\Pr\{yF_T \,|\, yD_T \cap \overline{xD_T}\} = \Pr\{yF_T \,|\, yD_T\}$ (from the probability of independent failures), and using Theorem 2, we derive the following development:

$$\begin{aligned}
\Pr\{NG_T \cap \overline{xD_T}\} &= \sum_{\substack{y \in S \\ y \neq x}} \Pr\{NG_T \cap yF_T \cap yD_T \cap \overline{xD_T}\} \\
&= \sum_{\substack{y \in S \\ y \neq x}} \Pr\{NG_T \cap yF_T \cap yD_T \cap \overline{xD_T}\} \\
&= \sum_{\substack{y \in S \\ y \neq x}} \Pr\left\{ \bigcap_{\substack{j=1 \\ x,y \notin MP^j}}^{p} \overline{MP_T^j} \cap yF_T \cap yD_T \cap \overline{xD_T} \right\} \\
&= \sum_{\substack{y \in S \\ y \neq x}} \left(\Pr\{yF_T \cap yD_T \cap \overline{xD_T}\} - \Pr\left\{ \left(\bigcup_{\substack{j=1 \\ x,y \notin MP^j}}^{p} MP_T^j \right) \cap yF_T \cap yD_T \cap \overline{xD_T} \right\} \right) \\
&\geq \sum_{\substack{y \in S \\ y \neq x}} \left(\Pr\{yF_T \,|\, yD_T\} \times \Pr\{yD_T\} \times \Pr\{\overline{xD_T}\} - \sum_{\substack{j=1 \\ x,y \notin MP^j}}^{p} \Pr\{MP_T^j \cap yF_T \cap yD_T \cap \overline{xD_T}\} \right)
\end{aligned}$$

□

3.4. *The Bound Algorithm (BA) for computing operational interruption rate indicators*

In this Subsection, we present recursive formulae for evaluating (lower and upper) bounds on probabilities of the three main events: NG_T (a No Go dispatch condition occurs during cycle *T*), ADM_T (the airline Accepts the Degraded Mode for take-off at the beginning of cycle *T+1*), and RDM_T (the airline Refuses the Degraded Mode for take-off at the beginning of cycle *T+1*) at each cycle *T*. These formulae derive from the recursive equation (4) of Subsection 3.1 and from the bounds provided by Theorems 3 and 4. These main event probability bounds can easily be computed from the given input data (including the given initial conditions at cycle 1, $\Pr\{xD_1\}$, for all component *x* in *S*.---see Subsection 2.2). From a straightforward application of Bayes rule, we obtain the following formulae:

$$UB(NG_T) = \sum_{x \in S} UB(NG_T | xF_T \cap xD_T) \times \Pr\{xF_T | xD_T\} \times UB(xD_T)$$

$$LB(NG_T) = \sum_{x \in S} LB(NG_T | xF_T \cap xD_T) \times \Pr\{xF_T | xD_T\} \times LB(xD_T)$$

$$UB(ADM_T) = \sum_{x \in S} \Pr\{ADM_T | \overline{NG_T} \cap xF_T \cap xD_T\} \times (1 - LB(NG_T | xF_T \cap xD_T)) \times \Pr\{xF_T | xD_T\} \times UB(xD_T)$$

$$LB(ADM_T) = \sum_{x \in S} \Pr\{ADM_T | \overline{NG_T} \cap xF_T \cap xD_T\} \times (1 - UB(NG_T | xF_T \cap xD_T)) \times \Pr\{xF_T | xD_T\} \times LB(xD_T)$$

$$UB(RDM_T) = \sum_{x \in S} (1 - \Pr\{ADM_T | \overline{NG_T} \cap xF_T \cap xD_T\}) \times (1 - LB(NG_T | xF_T \cap xD_T)) \times \Pr\{xF_T | xD_T\} \times UB(xD_T)$$

$$LB(RDM_T) = \sum_{x \in S} (1 - \Pr\{ADM_T | \overline{NG_T} \cap xF_T \cap xD_T\}) \times (1 - UB(NG_T | xF_T \cap xD_T)) \times \Pr\{xF_T | xD_T\} \times LB(xD_T)$$

where:

$$UB\left(NG_T \middle| xF_T \cap xD_T\right) = \sum_{i=1}^{k} \frac{\prod_{\substack{y \in MC^i \\ y \neq x}} UB\left(\overline{yD_T}\right)}{LB\left(xD_T\right)} \times 1_{\{x \in MC^i\}}$$

is obtained from inequality (5), and

$$LB\left(NG_T \middle| xF_T \cap xD_T\right) = 1 - \sum_{j=1}^{p} \prod_{y \in MP^j} UB\left(yD_T\right) \times 1_{\{x \notin MP^j\}}$$

is obtained from inequality (7).

The above bounds on the three main-event probabilities can be computed from input data, because $UB\left(\overline{xD_T}\right)$, $UB\left(xD_T\right)$, $LB\left(\overline{xD_T}\right)$, and $LB\left(xD_T\right)$ are easily obtained for all component x in S. Indeed, for $UB\left(\overline{xD_{T+1}}\right)$ and $LB\left(\overline{xD_{T+1}}\right)$, we have:

$$\begin{aligned} UB\left(\overline{xD_{T+1}}\right) \equiv\ & UB\left(\overline{xD_T}\right) - LB\left(NG_T \cap \overline{xD_T}\right) \\ & + \Pr\left\{ADM_T \middle| \overline{NG_T} \cap xF_T \cap xD_T\right\} \times \left(1 - LB\left(NG_T \middle| xF_T \cap xD_T\right)\right) \times \Pr\left\{xF_T \middle| xD_T\right\} \times UB\left(xD_T\right) \end{aligned}$$

and

$$\begin{aligned} LB\left(\overline{xD_{T+1}}\right) \equiv\ & LB\left(\overline{xD_T}\right) - UB\left(NG_T \cap \overline{xD_T}\right) \\ & + \Pr\left\{ADM_T \middle| \overline{NG_T} \cap xF_T \cap xD_T\right\} \times \left(1 - UB\left(NG_T \middle| xF_T \cap xD_T\right)\right) \times \Pr\left\{xF_T \middle| xD_T\right\} \times LB\left(xD_T\right), \end{aligned}$$

where:

$$UB\left(NG_T \cap \overline{xD_T}\right) \leq UB\left(\overline{xD_T}\right) \times \left(\sum_{\substack{y \in S \\ y \neq x}} \Pr\left\{yF_T \middle| yD_T\right\} \times \left(\sum_{i=1}^{k} \frac{\prod_{\substack{z \in MC^i \\ z \neq x \\ z \neq y}} UB\left(\overline{zD_T}\right)}{LB\left(yD_T\right)} 1_{\{y \in MC^i\}} \right) \right)$$

(using (6)), and

$$
\begin{aligned}
&LB\left(NG_T \cap \overline{xD_T}\right) \\
&\geq \sum_{\substack{y \in S \\ y \neq x}} \Pr\left\{yF_T \middle| yD_T\right\} \times LB\left(yD_T\right) \times LB\left(\overline{xD_T}\right) \\
&\quad - \sum_{\substack{y \in S \\ y \neq x}} \sum_{j=1}^{p} \left(\begin{array}{l} \min\left(\Pr\left\{yF_T \middle| yD_T\right\} \times \left(\prod_{z \in MP^j} UB\left(zD_T\right) \right) \times UB\left(yD_T\right), \Pr\left\{yF_T \middle| yD_T\right\} \times UB\left(\overline{xD_T}\right) \right) \\ \times 1_{\left\{y \notin MP^j\right\}} \times 1_{\left\{x \notin MP^j\right\}} \end{array} \right)
\end{aligned}
$$

(using (8)).

Now it remains to consider $UB\left(xD_T\right)$, and $LB\left(xD_T\right)$. Since

$LB\left(\overline{xD_T}\right) \leq \Pr\left\{\overline{xD_T}\right\} \leq UB\left(\overline{xD_T}\right)$, and because $\overline{xD_T}$ is the complement of xD_T, we have: $UB\left(xD_T\right) = 1 - LB\left(\overline{xD_T}\right)$ and $LB\left(xD_T\right) = 1 - UB\left(\overline{xD_T}\right)$.

The above-presented algorithm, that enables us to compute upper and lower bounds for the three main events NG, ADM, and RDM at each cycle, will be referred to in the sequel as the **Bound Algorithm (BA)**. The complexity of BA for a horizon of *T* cycles is $O\left(T.n^2\left(mL_c + pL_p\right)\right)$, where L_c is the maximum length of a minimal cut, and L_p is the maximum length of a minimal path. This complexity largely meets industrial computational time constraints for the systems considered in preliminary design.

Finally, remark that in our in-service aircraft reliability context, only upper bounds are crucial in guaranteeing system performance. Nevertheless, lower bounds can give indications on the maximal error of the upper-bound overestimation.

4. Computational experiments

In view of its industrial implementation, we have to evaluate the practical relevance of our Bound Algorithm (BA). We will compare the performance of BA with that of the Markov approach. The Markov approach has the advantage of providing the exact solution, allowing us to evaluate the precision of BA and its relative efficiency. Due to the excessive CPU time required by the Markov approach, we restrict this comparison to a horizon of 100 flight cycles. This horizon is sufficient for industrial validation purposes because, in practice, predictions in aircraft reliability generally do not consider horizons greater than 100 cycles.

For each application considered below, we start the process with all components working, i.e. $\Pr\{xD_1\} = 1$ for all x in S. We implemented both the BA and Markov approaches in MATLAB. We perform all computational experiments on a 256 Mb PC Pentium III running under Windows 2000 (except for some CPU-intensive runs of the Markov approach that are performed on a Sun SF6800 with 900 MHz CPU under Unix Solaris 8).

Let us now report numerical results on following applications: standard k-out-of-n:F system examples, a typical Air Data Inertial Reference System (with fictitious data), and an aircraft refuel system.

4.1 k-out-of-n:F systems

In this application, the components of each k-out-of-n:F systems are assumed to be of identical independent distributions. The worst-case complexity for k-out-of-n:F systems is: $O(n^3.2^n)$ for BA, against $O(n.4^n)$ for the Markov approach. We shall study all pairs (k,n) such that $2 \le k \le n \le 12$. These values cover a wide range of k-out-of-n aircraft

system instances. We choose $\Pr\{xF_T \mid xD_T\} = 10^{-4}$ for all component x in S, a typical component failure rate in aircraft reliability.

In the computational experiments that follow, averages are taken over 100 cycles (i.e. $T = 1,2...100$). Table 1 displays the average BA absolute error of the upper bound for $\Pr\{NG_T\}$ (probability of a No Go dispatch condition during cycle T). The maximal absolute error value of Table 1 is 5.3E-4. This error is not significant because it lies completely within the reliability bounds of data uncertainties. The analogous results on ADM_T and RDM_T are not presented because they derive directly from those on NG_T, and are even much better in terms of performance (precision). Our algorithm BA requires at most 258 seconds of CPU time, whereas the exact Markov approach needs up to 3,000 seconds.

Table 1. Absolute error of the upper bound for k-out-of-n:F systems

N =	2	3	4	5	6	7	8	9	10	11	12
k = 2	1.64E-08	3.08E-06	1.21E-05	2.94E-05	5.72E-05	9.74E-05	1.51E-04	2.21E-04	3.07E-04	4.11E-04	5.33E-04
k = 3		6.26E-08	3.88E-07	1.30E-06	3.23E-06	6.72E-06	1.24E-05	2.10E-05	3.32E-05	5.00E-05	7.22E-05
	k = 4		1.64E-09	1.10E-08	4.11E-08	1.15E-07	2.67E-07	5.47E-07	1.02E-06	1.77E-06	2.91E-06
		k = 5		3.82E-11	2.79E-10	1.15E-09	3.53E-09	8.95E-09	1.99E-08	4.01E-08	7.49E-08
			k = 6		8.24E-13	6.63E-12	3.00E-11	1.00E-10	2.75E-10	6.59E-10	1.43E-09
				k = 7		1.68E-14	1.48E-13	7.33E-13	2.65E-12	7.87E-12	2.03E-11
					k = 8		3.25E-16	3.16E-15	1.70E-14	6.65E-14	2.12E-13
						k = 9		5.75E-18	6.13E-17	3.57E-16	1.51E-15
							k = 10		4.17E-19	4.53E-18	2.68E-17
								k = 11		5.87E-21	6.95E-20
									k = 12		8.21E-23

4.2 Air Data Initial Reference System

To illustrate the efficiency of our BA algorithm, we consider a typical aircraft avionic system. The fault tree in Fig. 4 models it. It is a large system with 7 different types of components that correspond to 21 components, with 99 minimal cuts, and 3 minimal paths. Again, we choose $\Pr\{xF_T | xD_T\} = 10^{-4}$ for all component x in S. BA requires 26.84 seconds of CPU time to compute both $UB(NG_T)$ and $LB(NG_T)$ bounds. The Markov requires about 51 hours of CPU time.

Fig. 4. Fault tree modeling the No Go dispatch condition on Air Data Inertial Reference System

Table 2 displays the difference between both bounds and the exact Markov results as a function of the number of cycles. Obviously, the maximal error is obtained for 100 cycles. This maximal error of 1.45 % is completely satisfactory for predicting in-service aircraft reliability.

Table 2. Absolute error of the upper and lower bounds for the Air Data Inertial Reference System

Cycle T	1	2	3	10	30	50	70	100
$UB(NG_T) - \Pr\{NG_T\}$	0	1.14E-09	3.08E-09	3.79E-08	3.14E-07	7.90E-07	1.39E-06	2.43E-06
$LB(NG_T) - \Pr\{NG_T\}$	0	-1.34E-09	-3.87E-09	-5,37E-08	-4,74E-07	-1.23E-06	-2.25E-06	-4.12E-06

4.3 Aircraft refuel system

We consider a refuel system of an Airbus aircraft. Fig. 5 displays the associated fault tree involving the 15 different components. Here, we choose $\Pr\{xF_T | xD_T\} = 10^{-5}$ for all component x in S, a typical component failure rate in aircraft reliability.

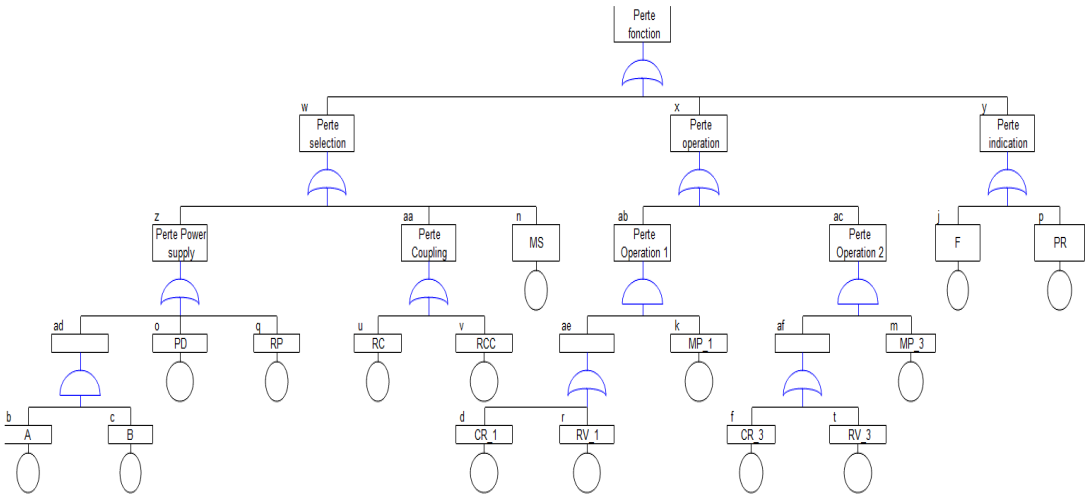

Fig. 5. Fault tree modeling the Airbus refuel system

After two weeks of operational use (100 cycles), BA obtained for $\Pr\{NG_T\}$ (with T=100) the following results: upper bound on the No Go event: $UB(NG_T)$ = 7.3E-5, and lower bound on the No Go event: $LB(NG_T)$ = 6.2E-5. Our BA method required 261 seconds of CPU time, whereas the Markov model needed around 2 hours (and yielded $\Pr\{NG_T\}$ = 6.5E-5). Again, due to real-world data uncertainties, this approximation is completely satisfactory for predicting in-service aircraft reliability. In particular, this Airbus refuel system case shows that BA is a promising method both in terms of precision and efficiency when applied to a real aircraft system.

5. Conclusion

In this paper, we introduced a general mathematical framework for modeling in-service aircraft reliability at the preliminary design stage. Then, we proposed an efficient algorithm (BA) to estimate operational interruption rate indicators which meets industrial computational time constraints for the systems considered in preliminary design. We demonstrated the precision of this method on real aircraft systems. Note that, all the results obtained in this paper can straightforwardly be extended to the aging effect case with an "as good as new" maintenance strategy. For the sake of simplicity, we restricted our presentation to an elementary set of maintenance tasks: "removal" and "damage tolerance". Current industrial implementation at Airbus does include other types of maintenance tasks (planned maintenance, preventive maintenance etc…).

Future related work will attempt at extending our approach (model and algorithm) to the broader problem of aircraft punctuality by computing the probability of operational interruption.

Acknowledgments

This research was prompted by Airbus, which provided the data. It was financially supported by Airbus and Agence Nationale pour la Recherche et la Technologie (ANRT).

Appendix A. Justification of Assumption A11:

$$\Pr\left\{\overline{xD_T} \cap \overline{yD_T}\right\} \le \Pr\left\{\overline{xD_T}\right\} \times \Pr\left\{\overline{yD_T}\right\}.$$

We shall show that this assumption is a direct consequence of the following two facts:

$$\Pr\left\{yD_T \middle| \overline{xD_T}\right\} > 0 \quad \text{and} \quad \Pr\left\{ yD_T \cap \left(\bigcup_{z \in S} zF_{T-1} \right) \right\} > 0, \qquad \text{(F1)}$$

$$\text{and} \qquad \sum_{z \in S} \Pr\left\{zF_{T-1}\right\} \le \frac{1}{M(T)(N(T)+1)}, \qquad \text{(F2)}$$

where:

$$M(T) := \max_{\substack{x,y,z \in S \\ y \ne x}} \left(\frac{\Pr\left\{yD_T \middle| zF_{T-1}\right\}}{\Pr\left\{yD_T \middle| \overline{xD_T}\right\}} \right) \text{ and } N(T) := \max_{y \in S} \left(\frac{\Pr\left\{ yD_T \cap \left(\bigcap_{z \in S} \overline{zF_{T-1}} \right) \right\}}{\Pr\left\{ yD_T \cap \left(\bigcup_{z \in S} zF_{T-1} \right) \right\}} \right).$$

Due to the high reliability of aircraft components, (F1) and (F2) are always verified in practice.

Proof of A11:

Using facts (F1) and (F2) above, we obtain the following inequalities:

$$
\begin{aligned}
\Pr\{yD_T\} &= \Pr\left\{ yD_T \cap \left(\bigcup_{z\in S} zF_{T-1} \right) \right\} + \Pr\left\{ yD_T \cap \left(\overline{\bigcup_{z\in S} zF_{T-1}} \right) \right\} \\
&\le (1+N(T))\Pr\left\{ yD_T \cap \left(\bigcup_{z\in S} zF_{T-1} \right) \right\} \\
&\le (1+N(T))\sum_{z\in S} \Pr\{yD_T \cap zF_{T-1}\} \\
&\le (1+N(T))\sum_{z\in S} \Pr\{yD_T \,|\, zF_{T-1}\}\Pr\{zF_{T-1}\} \\
&\le (1+N(T))M(T)\Pr\{yD_T \,|\, \overline{xD_T}\}\sum_{z\in S} \Pr\{zF_{T-1}\} \\
&\le \Pr\{yD_T \,|\, \overline{xD_T}\}.
\end{aligned}
$$

Then, from this last inequality, A11 is straightforward. □

References

1. E. Hugues, L. Saintis, A. Cabarbaye, ORA, model & tool for operational reliability prediction within Airbus, in *Proc. 14th Lambda-Mu Fiabilité Maintenabilité Conference*, Paris, 2004, pp 448-451.
2. E. Hugues, E. Charpentier, A. Cabarbaye, Application of Markov processes to predict aircraft operational reliability, in *Proc. 3rd European Systems Engineering Conference (EUSEC)*, Toulouse, 2002, pp. 231-235.
3. H. Guo, X. Yang, Automatic creation of Markov models for reliability assessment of safety instrument systems, Reliability Engineering and System Safety (2007), doi: 10.1016/j.ress.2007.03.029.
4. J. Banks, J.C Carson, B.L Nelson, D.M Nicol, *Discrete event system simulation* (Prentice Hall, 2000).
5. W.G Scheeweis, *A dynamic fault tree* (Lilole Verlag Gmbh, Hagen, Germany, 1999).
6. M. Cepin, B. Mavko, A dynamic fault tree, *Reliability Engineering and System Safety* **75** (2002), pp 83-91.
7. Y. Ma, KS. Trivedi, An algorithm for reliability analysis of phased-mission systems, *Reliability Engineering and System Safety* **66** (1999) pp 157-170.
8. S. Amari, G. Dill, E. Howald, A new Approach to solve dynamic fault trees, in *Proc. 49th RAMS*, Tampa Bay, 2003, pp. 374-379.
9. T. Khoda, K. Inoue, Probability evaluation of system-failure occurrence based on minimal cut-sets, in *Proc. 48th RAMS*, Seattle (USA), 2002, pp. 456-459.
10. L. Saintis, E. Hugues, C. Bès, M. Mongeau, Methods to asses the operational reliability of an aircraft system: Problem of dependency between component states, in *Proc. 15th Lambda-Mu Fiabilité Maintenabilité Conference*, Lille, 2006.
11. J.D. Esary, F. Proschan, Coherent structures of non-identical components, *Technometrics* **5** (1963), pp. 191-209.
12. M. Rausand, A. Hoyland, *System reliability theory* (John Wiley, 2004).